



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/559,259	04/27/2000	Hideyuki Hirano	1405.1020	2237

21171 7590 12/27/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER

REAGAN, JAMES A

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 12/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/559,259	Applicant(s) HIRANO ET AL.	
	Examiner James A. Reagan	Art Unit 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 August 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 and 5-26 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) 1-3, 5-24 and 26 is/are allowed.
- 6) ☐ Claim(s) 25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Status of Claims

1. This action is in response to the RCE filed on 15 August 2005.
2. Claim 4 has been cancelled.
3. Claims 1, 2, 7-15, 25, and 26 have been amended.
4. Claims 1-3 and 5-26 have been examined.

Information Disclosure Statement

5. The Information Disclosure Statement has been considered. An initialed copy of the Form 1449 is enclosed herewith.

Allowable Subject Matter

6. Claims 1-3 and 5-24, and 26 are allowed. See Reasons for Allowance under separate heading.

EXAMINER'S AMENDMENT

7. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.
8. Authorization for this examiner's amendment was given in a telephone interview with Mehdi D. Sheikerz on 16 September 2005.

9. The application has been amended as follows:

1. (CURRENTLY AMENDED) A data management method comprising:
extracting a portion of a digital content file to be distributed to prepare a preview sample as an index to the digital content file for representing the digital content file;
preparing a substantive file by encrypting the digital content file with a content key;
preparing user specific authorization information by encrypting the content key based upon user information;
preparing a user specific authorization information embedded preview sample by embedding the user specific authorization information, containing information for accessing the encrypted digital content file, as invisible information in the extracted preview sample;
synthesizing the substantive file and the user-specific-authorization-information-embedded preview sample to prepare a synthesized digital content file; and
distributing the synthesized digital content file.
2. (CURRENTLY AMENDED) The data management method set forth in claim 1, further comprising:
enabling access to the synthesized digital content file by separating the user-specific authorization information from the preview sample; and
restoring from the user-specific authorization information a decryption key as the content key for decrypting the substantive file.
3. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample is image data contained in the digital content file and at least one process among image processing, resizing, compressing and a y-compensation is executed on the image data

4. (CANCELLED)

5. (PREVIOUSLY PRESENTED) *The data management method set forth in claim 4, wherein the synthesized digital content file contains a plurality of substantive data files based on a plurality of digital content files, and contains a plurality of preview samples corresponding to the plurality of substantive data files; and wherein each preview sample is linked with respective corresponding ones of the plurality of substantive data files.*

6. (PREVIOUSLY PRESENTED) *The data management method set forth in claim 1, wherein the preview sample is data structuralized in one of JPEG and MPEG formats, and the synthesized digital content file is prepared by add-on synthesizing the substantive file to the preview sample using the format of the preview sample.*

7. (PREVIOUSLY PRESENTED) *The data management method set forth in claim 1, wherein in the preparing of the user-specific authorization information, the user information used in the encrypting of the content key is at least one of user identification information, equipment identification information loaded in user-employed computers, CPU identification information loaded in the user-employed computers, and identification information unique to digital-content-storing recording media.*

8. (PREVIOUSLY PRESENTED) *The data management method set forth in claim 1, wherein in the preparing of the user-specific authorization information, the user information used in the encrypting of the content key is identification information common to a plurality of users.*

9. (PREVIOUSLY PRESENTED) *The data management method set forth in claim 1, wherein in the preparing of the user-specific authorization information, the user information used in the encrypting of the content key is at least one of identification information unique to*

distributors of the digital content file, and identification information unique to authors of the digital content file.

10. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 7, wherein a decryption key for decrypting the encrypted user-specific authorization information is common to an encryption key as the content key for encrypting the digital content file, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.*

11. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 8 wherein a decryption key for decrypting the encrypted user-specific authorization information is common to an encryption key as the content key for encrypting the digital content file, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.*

12. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 9, wherein a decryption key for decrypting the encrypted user-specific authorization information is common to an encryption key as the content key for encrypting the digital content file, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.*

13. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 7, wherein digital content file distributors encrypt the content key employing a secret key as the user information, and the users decrypt the encrypted content key employing a public key provided in advance from the digital content file distributors, using public key cryptography.*

14. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 8, wherein digital content file distributors encrypt the content key employing a secret key as the user information, and the users decrypt the encrypted content key employing a public key provided in advance from the digital content file distributors, using public key cryptography.*

15. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 9, wherein digital content file distributors encrypt the content key employing a secret key as the user information, and the users decrypt the encrypted content key employing a public key provided in advance from the digital content file distributors, using public key cryptography.*

16. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample comprises as the invisible information a use count of times a user has used the digital content file; characterized in that the invisible information is rewritten each time a user uses the digital content file.*

17. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample comprises as the invisible information authorization information to enable use count control; characterized in that the invisible information is rewritten when a user uses the digital content file a predetermined number of times and more.*

18. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that the invisible information is rewritten on decrypting and reading the substantive file.*

19. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that the invisible information is rewritten when use of the digital content file is ended.*
20. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 17, characterized in that the invisible information is rewritten on decrypting and reading the substantive file.*
21. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 17, characterized in that the invisible information is rewritten when use of the digital content file is ended.*
22. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 16, wherein the invisible information in the preview sample comprises an error recovery function by containing redundant information.*
23. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that limits on read-out and use in decrypting the substantive file are governed based on the invisible information in the preview sample.*
24. *(PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that one of year, month, date, and time limits within which read-out and use is possible in decrypting the substantive file are governed based on the invisible information in the preview sample.*

25. (CURRENTLY AMENDED) A computer data signal embodied in a carrier wave, comprising protected provider data file synthesized with an extracted accessible sample as an index to the provider data file for representing the provider data file, the sample having watermarked data-authorization information of the provider and data-authorization information of a recipient protecting the data authorization information of the provider, thereby allowing a recipient system to preview the protected provider data file via the synthesized extracted accessible sample and access the protected provider data file according to the synthesized extracted accessible sample having the watermarked data-authorization information of the provider and the recipient.

26. (CURRENTLY AMENDED) An apparatus, comprising:
a programmed computer processor encrypting a content file with a content key, preparing user specific content authorization information by encrypting the content key based upon user information, embedding user specific content authorization information as a watermark in an extracted accessible sample, as an index to the content file for representing the content file and synthesizing the extracted accessible sample having the watermarked user-specific-content authorization information with the encrypted content file.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claim 25 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. *A computer data signal embodies in a carrier wave* is not tangibly embodied on a computer readable medium. As such, claim 25 merely recites computer code per se, not steps in a method/process, components of a system/apparatus, nor **computer executable program tangibly embodied on a computer readable medium comprising code or instruction** for executing the program claimed.

Reasons For Allowance

12. The following is an Examiner's statement of reasons for allowance:

None of the art of record, taken individually or combination, disclose at least the method step or system component of:

- *extracting a portion of a digital content file to be distributed to prepare a preview sample as an index to the digital content file for representing the digital content file;*
- *preparing a substantive file by encrypting the digital content file with a content key;*
- *preparing user specific authorization information by encrypting the content key based upon user information;*
- *preparing a user specific authorization information embedded preview sample by embedding the user specific authorization information, containing information for accessing the encrypted digital content file, as invisible information in the extracted preview sample;*

- *synthesizing the substantive file and the user-specific-authorization-information-embedded preview sample to prepare a synthesized digital content file;*

Independent Claims 1 and 26 are distinguished over the closest prior art of Stefik, which teaches embedding a watermark in a digital file that contains rights privileges (Abstract, column 12, lines 10-15). A review of entire Stefik reveals that Stefik discusses the "watermark data typically provides information relating to the owner of a document, the rights associated with that copy of the document and information relating to rendering event (e.g., when and where the document was printed). This information will typically aid in deterring or preventing unauthorized copying of the rendered work" (column 3, lines 22-39 and column 12, lines 10-51). However, Stefik fails to disclose or suggest other range of uses of watermark technology as well as location or integration of the watermark (see Stefik, column 10, line 66 to column 11, line 23). In other words, Stefik fails to disclose or suggest the claimed present invention's sample preview that has invisible authorization and index information for accessing the encrypted portion of the content.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

"Digital Watermarking and Tracking" (Jan. 26, 1998) discloses a digital watermarking technology.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** whose telephone number is **571.272.6710**. The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James Trammell** can be reached at **571.272.6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://portal.uspto.gov/external/portal/pair> . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

571-273-8300 [Official communications, After Final communications labeled "Box AF"]

571-273-8300 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window:**

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

JAMES A. REAGAN

Primary Examiner

Art Unit 3621

10 November 2005

